SailPoint

SOLUTION BRIEF

Securing Unstructured Data in Mergers & Acquisitions

In the past few years, we have seen a veritable explosion of mergers and acquisitions in the enterprise market. This is especially true for organizations in the healthcare and financial services industries. During this change, there may be something that anyone undergoing a merger or acquisition is missing: what happens with the data?

Mergers are complicated endeavors, and the scrutiny under which both companies will reside during the course of the change only increases the stress to keep what should be sensitive information protected. During the three phases of the implementation of the merger, from pre-approval to post-convergence, you need the right solution to keep your sensitive data secure.

Before the Merger

As most can assume, the documents pertaining to a merger or acquisition are extremely sensitive, especially before the change is approved. This is only complicated by the fact that a large part of this information is stored in unstructured data files (e.g., Word documents, PDFs, e-mails), where it has traditionally been difficult to secure access. When the details of a merger are leaked early, it can cause embarrassment for all parties involved, not to mention regulatory fines. Most impactful is that the merger may end up failing because of the leaked information. Controlling who knows about the merger and the sensitive details about it is key. You must be able to know where your merger documents are located, who has access to them and if they are overexposed, as well as who is accessing the documents and if that access is legitimate. Potential leaks are a major threat to the merger's success. If any of these questions cannot be quickly answered or threats dealt with in real time, you are putting the merger – and both companies – at risk.

During the Merger

Once the merger has been announced, the work isn't over. An assessment of the new company is vital. As it pertains to data, you need to be able to answer certain questions:

- What data are they bringing with them?
- What can be removed/left behind?
- Where is their sensitive data? Do you need to take special precautions for it? Is any of it stored in the cloud?
- What permissions structure do they have? Who has administrative access?
- Who are the business owners of the documents?
- What is their current solution, if any, for managing the entitlements and authentications for accessing their data?

Before everything is assimilated, you need to review and clean up the permissions on high-risk data. Many organizations have a vast amount of over-entitled users and data can be too easily accessed. Your goal during the merger is to bring in the data, but leave behind the risk.

After the Merger

The day after the merger, the amount of data you have is going to skyrocket very suddenly. But as soon as the merger is complete, you can expect that type of growth overnight. Your top concern at that point is to secure access for all the data the enterprise just acquired and now possesses and ensure it is complying with regulatory requirements.

60%

Estimated yearly growth for enterprise unstructured data[1]

However, this is not an easy venture and can pose significant challenges. Manual methods of securing the data have a very low chance of actual success; automation is the key. You must be able to create the roles, policies and procedures necessary and have those rules put into effect without needing to go through one-by-one to change and manage permissions.

Maintaining the high level of security around your data can also be a struggle. Change is difficult and doing things "the old way" may sometimes creep into your processes. Once all the data has been assimilated and given the proper permissions, automating the oversight of the data is key. You need a solution that can:

- Identify the correct business owners to certify and maintain the correct access to your data.
- Increase efficiency through automation and self-service tools.
- Provide IT the needed oversight on managed locations.
- Locate and track sensitive data to ensure it is not overexposed or improperly accessed.
- Provision access to new data and storage locations as they are created.

[1] *IDC: Unstructured data will become the primary task for storage,* TechTarget

SailPoint Can Help

At SailPoint, we know how to secure an organization's identities, including how (or if) they access your data. In order for your organization to be secure, you need both identity governance and data access governance solutions that ensure you have full visibility, control and compliance over your data.

Visibility

In order to govern users' access to data, you must have a holistic view across your entire infrastructure. If your IT team or business owners cannot see all the permissions a user has, they simply cannot make the right decisions about who should have access to what to avoid complications from over-entitlement and separation-of-duty (SoD).

IdentityIQ File Access Manager helps answer these essential questions:

- Where is your sensitive information?
- Who has access to it and is that access too broad?
- What are those users doing with their access, and do these actions violate your security policy?
- Can you prove all this to an auditor?

Control

Before you can effectively control and secure your organization's data, you must first identify its owners. While structured data stores have generally been assigned business owners, unstructured data usually do not have a complementary owner. Without proper data owners, unstructured data in files can be easily overlooked, incorrectly classified and improperly managed in terms of who has access.

Organizations who fail to actively assign accountability to data owners to understand who should have access and who does have access to sensitive data in the enterprise are leaving themselves open to data breaches and regulatory penalties. For instance, if a public company has its financial data leaked and its stock price falls as a result, its investors are negatively affected and the company is now in violation of the Sarbanes-Oxley (SOX) regulations.

Once the owners have been elected from those who actually use the data on a regular basis, you must then enable them to manage their data via user-friendly tools that ultimately save them time.

IdentityIQ File Access Manager allows data owners to:

- Get visibility over the data they own.
- Self-configure alerts that are brought directly to their attention.
- Create a task list to keep owners on track.
- Provide controlled access through self-service access requests.
- Give IT oversight and compliance through periodic entitlement reviews.
- Add access and remove high-risk access through actionable intelligence.

Compliance

Organizations in a regulated industry will always be concerned with staying within compliance. But even those in less-regulated industries still need to understand that the merger data they possess is essentially intellectual property that is time-sensitive. The security of this sensitive information and compliance with any regulations is imperative throughout the merger process.

IdentityIQ File Access Manager helps compliance efforts by providing:

- Visibility into the location of merger documents.
- Validation that merger documents are only accessible on a need-to-know basis.
- Activity monitoring to ensure that only the proper identities are accessing the data.

Conclusion

Mergers and acquisitions can be cumbersome creatures, taking years to complete. The unstructured data that these assimilations bring with them can be simply staggering. Securing the information not only about the merger itself, but also the rest of the sensitive information both companies possess is essential to its success. SailPoint can help to ensure your data stays secure through the entire merger lifecycle and beyond.